AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer implemented system that facilitates an application to produce a response to an authentication challenge, comprising the following computer executable components:

a learning component that determines anticipated authentication challenges to resource requests from applications based upon run-time learning during previous resource requests by applications;

an authentication manager that receives first data associated with the communication challenge and processes the first data into second data of a first type appropriate for a first authentication module, ~~the authentication manager further processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for second data,~~ the authentication manager further communicates ~~at least one of~~ the second data to at least one authentication module, the authentication manager further communicates the second data to the at least one different authentication module if the first module is unable to process the authentication challenge, the second data is related to the first data and the authentication challenge, the authentication manager also generates pseudo-challenges and communicates data to at least one authentication module; and

at least one authentication module that receives the ~~at least one~~ second data from the authentication manager and produces third data related to responding to the authentication challenge.

2. (Previously Presented) The system of claim 1, comprising a cache that stores one or more third data related to responding to the authentication challenge.

3. (Previously Presented) The system of claim 2, wherein the authentication manager receives a set of first data associated with a multipart authentication challenge, to process the set of first data into a set of the second data, and communicates the set of second data to at least one authentication module, the set of second data is related to the set of first data and the multipart authentication challenge.

4. (Previously Presented) The system of claim 3, wherein the at least one authentication module receives the set of second data from the authentication manager and produces a set of third data related to responding to the multipart authentication challenge.

5. (Previously Presented) The system of claim 4, wherein the cache stores a set of third data related to responding to the multipart authentication challenge.

6. (Previously Presented) The system of claim 2, wherein:

the authentication manager accepts a pre-authentication challenge test message associated with an anticipated authentication challenge, processes the test message into a pre-authentication challenge test data, and communicates the pre-authentication challenge test data to at least one authentication module, the pre-authentication challenge test data related to the pre-authentication challenge test message;

at least one authentication module receives the pre-authentication challenge test data from the authentication manager and produces a pre-authentication challenge test response data related to responding to the pre-authentication challenge test message; and

the cache stores one or more pre-authentication challenge test response data related to responding to the pre-authentication challenge test message, the cache selectively provides the pre-authentication challenge test response data upon request by the authentication manager.

7. (Previously Presented) The system of claim 6, wherein the authentication modules employ one or more services.

8. (Previously Presented) The system of claim 1, comprising:

a class factory, the class factory selectively instantiates one or more authentication objects based, at least in part, on the first data, and

the class factory makes the one or more instantiated authentication objects callable by the authentication manager.

9. (Previously Presented) The system of claim 8, comprising:

a data store that holds information associated with selectively instantiating the one or more authentication objects, the data store further holds information associated with making the one or more instantiated authentication objects callable by the authentication manager.

10. (Previously Presented) The system of claim 9, comprising:

a registrar that registers an authentication object with the class factory.

11. (Previously Presented) The system of claim 10, wherein the registrar registers an authentication object with the data store.

12. (Previously Presented) The system of claim 11, wherein the application does not have to be recoded or recompiled to employ the registered authentication object.

13. (Previously Presented) The system of claim 1, wherein one or more authentication objects generate the third data associated with responding to an authentication challenge associated with at least one of, a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

14. (Previously Presented) The system of claim 1, wherein the authentication manager and the one or more authentication objects are distributed to one or more computers.

15. (Previously Presented) The system of claim 11, wherein the class factory, the data store and the registrar are distributed to one or more computers.

16. (Currently Amended) A computer implemented method for enabling an application to produce a response to an authentication challenge, comprising:

anticipating an authentication challenge to a resource request from an application based upon run-time machine learning during previous resource requests by applications;

pre-authenticating the resource request by generating and storing an authentication response to the anticipated authentication challenge;

generating a pseudo-challenge and storing a response to the pseudo-challenge;

employing a component implemented on a computer readable medium to accept the authentication challenge;

passing a first data associated with the authentication challenge to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module if the first module is unable to process the authentication challenge, the first and second authentication modules having different requirements for the second data;

passing at least one of the second data associated with the authentication challenge or pseudo-challenge to one or more authentication modules, where the authentication modules are registered with the authentication manager, registering the modules includes informing the authentication manager of which system authentication challenges the module is capable of processing and where the authentication modules are operatively connected to the authentication manager; and

producing one or more responses to the authentication challenge.

17. (Original) The system of claim 16, comprising:

caching one or more responses to the authentication challenge; and

retrieving a response from the cached responses.

18. (Original) The method of claim 16, wherein the authentication challenge is generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

19. (Original) The method of claim 16, wherein one or more authentication modules can be created and registered after the receipt of one or more authentication challenges.

20. (Previously Presented) A computer readable medium, comprising:

computer executable instructions that perform the method of claim 19.

21. (Cancelled).

22. (Currently Amended) A computer implemented method for enabling an application to produce a response to an authentication challenge, comprising:

generating a pre-authentication challenge test message based upon anticipating an authentication challenge to a resource request from an application based upon run-time learning during previous resource requests by applications;

generating a pseudo-challenge message and storing a response to the pseudo-challenge;

utilizing a component implemented on a computer readable medium to pass a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for second data;

passing at least one of the second data associated with the pre-authentication challenge test message to an appropriate ~~one or more~~ authentication module, if the module is unable to process the challenge passing the at least one of the second data to the at least one different authentication module ~~modules~~, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;

producing one or more responses to the pre-authentication challenge test message; and

caching the one or more responses to the pre-authentication challenge test message.

23. (Original) The method of claim 22, wherein the pre-authentication challenge test message is related to an authentication challenge generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

24. (Original) The method of claim 22, wherein one or more authentication modules can be created and registered after the generation of one or more pre-authentication challenge test messages.

25. (Previously Presented) The method of claim 22, wherein the application does not have to be recoded or recompiled to employ the one or more created and registered authentication modules.

26. (Currently Amended) A computer readable medium having computer executable instructions operable to perform a method comprising:

generating a pre-authentication challenge test message based upon anticipating an authentication challenge to a resource request from an application based upon run-time learning during previous resource requests by applications;

generating a pseudo-challenge and storing a response to the pseudo-challenge;

passing a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for second data;

employing a component implemented on a computer readable medium to pass at least one of the second data associated with the pre-authentication challenge test message to an appropriate authentication module, if the module is unable to process the challenge, passing the test message to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;

producing one or more responses to the pre-authentication challenge test message; and

caching the one or more responses to the pre-authentication challenge test message.

27. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to selecting an authentication object to process data associated with an authentication challenge.

28. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to registering an authentication object with a class factory and a data store, wherein registering the authentication object facilitates an authentication manager employing the authentication object to produce a response to an authentication challenge.

29. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing a response to an authentication challenge, where the response was generated by an authentication module adapted to receive data from an authentication manager and to send the response to the authentication manager.

30. (Currently Amended) A system enabling an application to respond to a challenge to a request to access a resource addressable by a URI, comprising:

~~anticipating~~ means for anticipating an authentication challenge to a resource request from an application based upon run-time learning during previous resource requests by applications

~~receiving~~ means for receiving the challenge, the receiving means separate from the application;

~~distributing~~ means for processing data associated with the challenge into second data of a first type appropriate for a first authentication module and second data of a second type appropriate for a second authentication module and distributing at least one of the second data to appropriate producing means, if the first producing means is unable to process the challenge, distributing the at least one of the second data to one or more producing means, the distributing means being separate from the application, the first and second authentication modules having different requirements for second data;

~~producing~~ means for producing a response to the challenge; the producing means being separate from the application; and

~~storing~~ means for storing a response to the challenge.